

Methods and apparatus for a computer network firewall with multiple domain support

Patent Number: ☐ EP0909074
Publication date: 1999-04-14
Inventor(s): COSS MICHAEL JOHN (US); MAJETTE DAVID L (US); SHARP RONALD L
Applicant(s): LUCENT TECHNOLOGIES INC (US)
Requested Patent: ☐ JP11168511
Application: EP19980306998 19980901
Priority Number(s): US19970927382 19970912
IPC Classification: H04L29/06
EC Classification: H04L29/06, H04L29/06C6A
Equivalents:

Abstract

The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-168511

(43) 公開日 平成11年(1999) 6月22日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 12/66

H 0 4 L 11/20

B

G 0 6 F 13/00

3 5 1

G 0 6 F 13/00

3 5 1 Z

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 E

H 0 4 L 9/32

H 0 4 L 9/00

6 7 3 B

6 7 3 A

審査請求 未請求 請求項の数26 O L (全 18 頁)

(21) 出願番号 特願平10-252832

(22) 出願日 平成10年(1998) 9月7日

(31) 優先権主張番号 08/927382

(32) 優先日 1997年9月12日

(33) 優先権主張国 米国 (US)

(71) 出願人 596077259

ルーセント テクノロジーズ インコーポ
レイテッドLucent Technologies
Inc.アメリカ合衆国 07974 ニュージャージ
ー、マレーヒル、マウンテン アベニュー
600-700

(72) 発明者 マイケル ジョン コス

アメリカ合衆国, 08807 ニュージャージ
ー、ブリッジウォーター、ウェックスフォ
ード ウェイ 28

(74) 代理人 弁理士 三俣 弘文

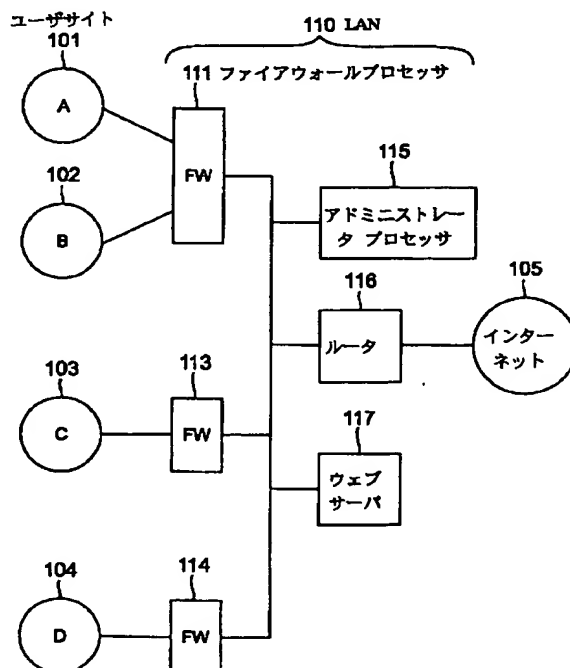
最終頁に続く

(54) 【発明の名称】 パケット検証方法

(57) 【要約】

【課題】 単一のファイアウォールが、それぞれ別々のセキュリティポリシーを有する複数のユーザをサポートすることを可能にする。

【解決手段】 ファイアウォールは、パケットに対するセッションキーを導出し、セッションキーに基づいて複数のセキュリティポリシーのうちから少なくとも1つのセキュリティポリシーを選択し、選択されたセキュリティポリシーを用いてパケットを検証する。実施例では、セッションキーはパケットのヘッダ情報から導出される項目を含む。この項目としては、例えば、IPソース/デスティネーションアドレス、次のレベルのプロトコル、該プロトコルに関係づけられたソース/デスティネーションポートがある。また、次のレベルのプロトコルは、例えば、TCPまたはUDPである。セキュリティポリシーは、相異なるグループ、あるいは、与えられたグループ内の相異なるサブグループに対応する。



【特許請求の範囲】

【請求項1】 コンピュータネットワークにおけるパケットを検証する方法において、該方法は、前記パケットに対するセッションキーを導出するステップと、前記セッションキーの関数として複数のセキュリティポリシーのうちから少なくとも1つのセキュリティポリシーを選択する選択ステップと、選択されたセキュリティポリシーを用いて前記パケットを検証するステップとからなることを特徴とするパケット検証方法。

【請求項2】 前記セッションキーは、前記パケット内のデータに付加されるヘッダ情報から導出される項目を含むことを特徴とする請求項1に記載の方法。

【請求項3】 前記セッションキーは、
(i) ソースアドレス、
(ii) デスティネーションアドレス、
(iii) 次のレベルのプロトコル、
(iv) プロトコルに関係づけられたソースポート、および
(v) 該プロトコルに関係づけられたデスティネーションポート、
からなるセットからの少なくとも1つの項目を含むことを特徴とする請求項1に記載の方法。

【請求項4】 前記セッションキーは、
(i) インターネットプロトコル（以下「IP」という。）ソースアドレス、
(ii) IPデスティネーションアドレス、
(iii) 次のレベルのプロトコル、
(iv) 該プロトコルに関係づけられたソースポート、および
(v) 該プロトコルに関係づけられたデスティネーションポート、
からなるセットからの少なくとも1つの項目を含むことを特徴とする請求項1に記載の方法。

【請求項5】 前記次のレベルのプロトコルは、伝送制御プロトコルTCPまたはユーザデータグラムプロトコルUDPであることを特徴とする請求項3に記載の方法。

【請求項6】 前記ネットワークは複数のネットワークインタフェースを含み、前記選択ステップは、要求が受信されたインタフェースを判定するステップを含むことを特徴とする請求項1に記載の方法。

【請求項7】 前記ネットワークは複数のネットワークインタフェースを含み、前記選択ステップは、要求の送信先のインタフェースを判定するステップを含むことを特徴とする請求項1に記載の方法。

【請求項8】 コンピュータネットワークにおけるパケ

ットを検証する方法において、該方法は、それぞれアクセスルールのセットを含む複数の独立のセキュリティポリシーを指定するステップと、前記パケットにはいずれのセキュリティポリシーが適当であるかを判定するステップと、判定されたセキュリティポリシーのアクセスルールのセットを用いて前記パケットを検証するステップとからなることを特徴とするパケット検証方法。

【請求項9】 複数のセキュリティポリシーの少なくとも一部は、単一のファイアウォールに関連づけられた相異なるグループに対応することを特徴とする請求項8に記載の方法。

【請求項10】 複数のセキュリティポリシーの少なくとも一部は、与えられたグループ内の相異なるサブグループに対応することを特徴とする請求項8に記載の方法。

【請求項11】 与えられたグループのアドミニストレータのみが、該グループのセキュリティポリシーのルールを修正する権限を有することを特徴とする請求項8に記載の方法。

【請求項12】 コンピュータネットワークのファイアウォールでパケットを検証する際に用いられる装置において、前記ファイアウォールは複数の独立のセキュリティポリシーを指定し、各セキュリティポリシーはアクセスルールのセットを含み、前記装置は、前記ファイアウォールにおいて、(i) 前記パケットにはいずれのセキュリティポリシーが適当であるかを判定し、(ii) 判定されたセキュリティポリシーのアクセスルールのセットを用いて前記パケットを検証する、プロセッサを有することを特徴とする、パケットを検証する際に用いられる装置。

【請求項13】 複数のセキュリティポリシーの少なくとも一部は、単一のファイアウォールに関連づけられた相異なるグループに対応することを特徴とする請求項12に記載の装置。

【請求項14】 複数のセキュリティポリシーの少なくとも一部は、与えられたグループ内の相異なるサブグループに対応することを特徴とする請求項12に記載の装置。

【請求項15】 与えられたグループのアドミニストレータのみが、該グループのセキュリティポリシーのルールを修正する権限を有することを特徴とする請求項12に記載の装置。

【請求項16】 コンピュータネットワークにおけるファイアウォールを提供する方法において、該方法は、アクセスルートを複数のドメインに分割するステップと、与えられたドメインのアドミニストレータのみが該ドメ

インのセキュリティポリシーのルールを修正する権限を有するように前記アクセスルールを管理するステップとからなることを特徴とする、ファイアウォールを提供する方法。

【請求項17】 コンピュータネットワークにおけるパケット検証を行うコンピュータシステムにおいて、該コンピュータシステムは、セッションを求める要求から少なくとも1つのデータ項目を取得する手段と、前記データ項目の関数として複数のセキュリティポリシーのうちから少なくとも1つのセキュリティポリシーを選択する選択手段と、選択されたセキュリティポリシーを用いて前記セッションのパケットを検証する手段とからなることを特徴とするコンピュータシステム。

【請求項18】 前記ネットワークは複数のネットワークインタフェースを含み、前記選択手段は、要求が受信されたインタフェースを判定する判定手段を含むことを特徴とする請求項17に記載のコンピュータシステム。

【請求項19】 前記判定手段は、前記要求に含まれるソースIPアドレスを参照する手段を含むことを特徴とする請求項18に記載のコンピュータシステム。

【請求項20】 前記ネットワークは複数のネットワークインタフェースを含み、前記選択手段は、要求の送信先のインタフェースを判定する判定手段を含むことを特徴とする請求項17に記載のコンピュータシステム。

【請求項21】 前記判定手段は、前記要求に含まれるデスティネーションIPアドレスを参照する手段を含むことを特徴とする請求項20に記載のコンピュータシステム。

【請求項22】 コンピュータネットワークにおけるパケット検証方法において、該方法は、セッションを求める要求から少なくとも1つのデータ項目を取得するステップと、前記データ項目の関数として複数のセキュリティポリシーのうちから少なくとも1つのセキュリティポリシーを選択する選択ステップと、選択されたセキュリティポリシーを用いて前記セッションのパケットを検証するステップとからなることを特徴とするパケット検証方法。

【請求項23】 前記ネットワークは複数のネットワークインタフェースを含み、前記選択ステップは、要求が受信されたインタフェースを判定する判定ステップを含むことを特徴とする請求項22に記載の方法。

【請求項24】 前記判定ステップは、前記要求に含まれるソースIPアドレスを参照するステップを含むことを特徴とする請求項23に記載の方法。

【請求項25】 前記ネットワークは複数のネットワークインタフェースを含み、

前記選択ステップは、要求の送信先のインタフェースを判定する判定ステップを含むことを特徴とする請求項22に記載の方法。

【請求項26】 前記判定ステップは、前記要求に含まれるデスティネーションIPアドレスを参照するステップを含むことを特徴とする請求項25に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータネットワークにおける権限のないアクセスの防止に関し、特に、コンピュータネットワーク内のファイアウォール保護に関する。

【0002】

【従来の技術】コンピュータネットワークでは、情報は、通常、パケットの形で伝送される。あるサイトにある情報は、そのサイトまたは別のサイトのコマンドで、別のサイトからアクセスされ、あるいは、別のサイトへ送信される。従って、例えば情報が財産である場合、権限のないアクセスに対する保護の必要がある。このために、ファイアウォールとして知られるワークプロセッサコンポーネントで実行される、パケットフィルタリングという技術が開発され市販されている。ファイアウォールでは、パケットは検査されフィルタリングされる。すなわち、あらかじめ定義されたアクセスルールのセットに従っているかどうかに応じて、パケットは、通過し、あるいは、廃棄される。通常、このルールセットは表形式で表される。

【0003】一般に、ファイアウォールアドミニストレータは、ファイアウォールの一方の側から他方の側へは、同意された広範なアクセスを許容するが、アクティブなネットワークセッションの一部ではない逆向きの伝送は遮断する。例えば、会社の「内部」の従業員はファイアウォールを通じてインターネットのような「外部」のネットワークに無制限にアクセスすることができるが、インターネットからのアクセスは、特別に権限を与えられていなければ遮断される。このような、会社とインターネットの境界にあるファイアウォールに加えて、ファイアウォールは、ネットワークドメイン間にも置かれることがあり、また、ドメイン内でも、サブドメインを保護するために用いられることがある。それぞれの場合において、異なるセキュリティポリシーが関係している。

【0004】いくつかの複雑なネットワークプロトコルでは、外部からユーザへ戻る別個の追加のネットワークセッションが必要とされる。そのような複雑なプロトコルの1つは、RealAudioという商品名で知られているサービスによって用いられている。特別の処置がなければ、この別個のセッションに対する要求はファイアウォ

ールによって遮断されてしまう。

【0005】このような複雑なプロトコルに対して、ユーザの代わりにファイアウォールプロセス上で並行して走る別個の「プロキシ」プロセスが開発されている。プロキシプロセスは、別の特殊目的アプリケーション、例えば、認証、メール処理、およびウィルススキャンのようなサービスを実行するためにも、開発されている。

【0006】

【発明が解決しようとする課題】ファイアウォールプロセスが並行プロセスをサポートする容量には限界があるので、並行して走らせることができるセッションの数を最大にするためには、ファイアウォール上のプロキシプロセスに対する需要を最小にすることが好ましい。さらに、このような最小化は、全伝送レートに関しても、好ましい。その理由は、入力データが別々のプロセスを通ると伝送が遅くなるためである。

【0007】

【課題を解決するための手段】本発明は、処理効率を改善し、セキュリティを改善し、アクセスルール自由度を増大させ、複雑なプロトコルを扱うファイアウォールの能力を高めるように、コンピュータネットワークのファイアウォールを実現する技術を提供する。本発明の第1の特徴によれば、コンピュータネットワークファイアウォールは、与えられたパケットに対していくつかの別個のアクセスルールセットのうちのいずれかを適用することによって、(a) 複数のセキュリティポリシー、(b) 複数のユーザ、または、(c) 複数のセキュリティポリシーおよび複数のユーザの両方をサポートすることができる。パケットに対して適用されるルールセットは、入出力ネットワークインタフェースや、ネットワークのソースおよびデスティネーションのアドレスのような情報に基づいて決定される。

【0008】本発明の第2の特徴によれば、コンピュータネットワークファイアウォールは、パケットに適用されるルール処理の結果を記憶することによって性能を改善する「状態付き」パケットフィルタリングを利用するように構成される。状態付きパケットフィルタリングは、パケットに対するルール処理結果をキャッシュし、キャッシュされた結果を利用して後続の同種のパケットに対するルール処理を迂回することによって実現される。例えば、あるネットワークセッションの特定のパケットにルールセットを適用した結果をキャッシュし、同じネットワークセッションからの後続のパケットがファイアウォールに到着したときに、キャッシュされている前のパケットからの結果を、その後続パケットに対して用いる。これにより、それぞれの入力パケットにそのルールセットを適用する必要がなくなる。

【0009】本発明の第3の特徴によれば、コンピュータネットワークファイアウォールは、ソースホストアドレス、デスティネーションホストアドレス、およびサ-

ビスタイプのようなセッションデータ項目に基づいて設定することが可能な依存関係マスクを用いて、ネットワークセッションを認証あるいは阻止する。依存関係マスクを用いて、ファイアウォールによって処理されているアクティブセッションのキャッシュに問合せをすることが可能であり、それにより、問合せを満たすセッションの数を識別することができる。この問合せを、アクセスルールに対応させ、特定のルールのセッションが、その問合せに適合する数に依存するようにすることが可能である。

【0010】本発明の第4の特徴によれば、コンピュータネットワークファイアウォールは、パケットを処理するためのアクセスルールのセットに追加された動的ルールを利用することが可能である。動的ルールによれば、与えられたルールセットは、ルールセット全体をリロードすることを要求せずに、ネットワークにおいて起こるイベントに基づいて修正される。動的ルールの例としては、単一のセッションに対してのみ用いられる「ワンタイム」ルール、指定された期間に対してのみ用いられる時限ルール、および、ある条件が満たされたときのみ用いられるしきい値ルールがある。他のタイプの動的ルールとしては、ホストグループを定義するルールがある。この動的ルールによれば、アクセスルールセットの他の事項を変更せずに、ホストを追加あるいは削除するようにホストグループを変更することができる。

【0011】本発明の第5の特徴によれば、アプリケーションプロキシのファイアウォールの負担を軽減するように、処理のための別のサーバにネットワークセッションをリダイレクトするようコンピュータネットワークファイアウォールに対して指令することができる。この別サーバは、リダイレクトされたネットワークセッションを処理した後、そのセッションを、ファイアウォールを通じて、もとの意図されたデスティネーションへ渡す。

【0012】本発明のコンピュータネットワークファイアウォールにより、広範囲の重要なアプリケーションでのファイアウォール処理が可能となる。例えば、本発明は、ダイヤルアップアクセスゲートウェイに実装可能である。本発明の別の実施例では、ファイアウォールの第1部分がネットワークに存在し、ファイアウォールの第2部分がセットトップボックス、コンピュータあるいはその他の、家庭または会社にあるユーザ端末にあるというように分散的にも実装可能である。後者の実施例によれば、本発明のファイアウォール技術は、例えば、家庭においてインターネットとビデオアクセスの親による制御を提供することが可能である。

【0013】

【発明の実施の形態】ファイアウォールにおいて、例えば、別個のローカルエリアネットワーク(LAN)間あるいはLANのサブネット間でのデータの流れを制御する好ましい技術が実現される。以下で、本発明の実施例

は、プロセスに関して説明する。このようなプロセスの効率的なプロトタイプは、汎用PCハードウェア上に実装するためにプログラミング言語Cを用いて、コンピュータシステムソフトウェアとして実現されている。専用のファームウェアあるいはハードウェアのコンピュータシステム実装により、さらに効率を向上させることも可能である。

【0014】1. 複数のセキュリティドメインのサポート

複数のセキュリティドメインをサポートする能力により、単一のファイアウォールが、それぞれ別々のセキュリティポリシーを有する複数のユーザをサポートすることが可能となる。また、相異なるセキュリティポリシーをサブサイト間の通信に適用することができるため、このような能力は、サイト内でも使用可能である。それぞれの構成を図1および図2に例示する。

【0015】図1に、インターネット105への接続にファイアウォールを有する4つのユーザサイト101～104（例として、会社A～D）を示す。このような保護は、ファイアウォール設備によって提供される。ファイアウォール設備は、ここではLAN110の形態であり、ファイアウォールプロセッサ111、113および114、アドミニストレータプロセッサ115、ルータ116ならびにウェブサーバ117を有する。ファイアウォールプロセッサ113および114はそれぞれ単一のサイト（すなわち、それぞれサイト103および104）専用である。ファイアウォールプロセッサ111は、2つのサイト101および102にサービスするように設定される。ファイアウォールプロセッサ111は、2つのサイトそれぞれとインターネット105との間、および、2つのサイト間の通信に、別々のファイアウォールポリシーを実装する。ファイアウォールプロセッサ111の好ましい動作のためのプロセスについて、複数のファイアウォールポリシーのうちからの適切な選択を含めて、図5および図6を参照して後述する。

【0016】図2に、ファイアウォールプロセッサ211を通じてインターネット105に接続されたユーザサイト201を示す。アドミニストレータプロセッサ215およびルータ216は、ファイアウォールプロセッサ211に接続される。ルータ216は、ユーザサイト201の内部にある別のファイアウォールプロセッサ212および213に接続される。ファイアウォールプロセッサ212は、単一のサブサイト223（例として人事（HR））を保護する。ファイアウォール213は、2つのサブサイト（例として、給与（P）および支払（D））を、サイト201の残りの部分に対して、および、サブサイト221と222の間の通信に関して、保護するように設定される。これは、ファイアウォールプロセッサ213において、図5および図6で例示されるプロセスを用いることによって達成される。

【0017】セキュリティポリシーは、アクセスルールのセットによって表現される。アクセスルールのセットは、表（テーブル）形式で表され、ファイアウォールアドミニストレータによってファイアウォールにロードされる。図3に示すように、このようなテーブルは、ルール番号、ソースおよびデスティネーションのホストの名称、パケットで要求されることが可能な特殊サービスの名称、および、パケットに対してなされるアクションの指定を含むカテゴリに対して与えられる。特殊サービスには、例えば、プロキシサービス、ネットワークアドレス翻訳、および、暗号化が含まれる。図3では、「ソースホスト」、「デスティネーションホスト」および「サービス」というカテゴリは、パケットに対して指定されたアクションがなされるために、そのパケットに含まれるデータが満たさなければならない条件を課している。他の条件を含めることも可能であり、そのような条件は、必ずしも、パケットに含まれるデータに関係する必要はない。例えば、ルールの適用は、日時に関して条件づけられることも可能である。

【0018】あるルールにおいて、ルールテーブルに与えられたカテゴリが無関係である場合、対応するテーブルエントリは「ワイルドカード」とマークされる。これは、任意のカテゴリあるいはカテゴリの組合せに適用可能である。図3などでは、ワイルドカードエントリにアスタリスク（*）を用いている。「FTP」はファイル転送プロトコル（file transfer protocol）を表す。

【0019】パケットに対するルール処理において、パケットによって満たされるルールが見つかるまで（または、ルールテーブルの最後まで。その場合、そのパケットは廃棄される。）、ルールは順に適用される。ルールを満たすパケットに対して、そのルールに含まれる各条件が満たされなければならない。例えば、図3において、ソースホストAからデスティネーションホストDへの、メールを表すパケットは、ルール20により廃棄される。以下は、本発明による例示的なルールセットカテゴリのさらに詳細なリストである。最初の5個のカテゴリ名は、図3のカテゴリに対応する。

【0020】カテゴリ名：ルール番号

説明：ドメイン内のルールの番号。ルール番号は、一意である必要はないが、一般に、単一のサービス（例えばFTP）を表すべきである。

【0021】カテゴリ名：ソースホスト

説明：ソースホストグループの識別子またはIPアドレス。

【0022】カテゴリ名：デスティネーションホスト

説明：デスティネーションホストグループの識別子またはIPアドレス。

【0023】カテゴリ名：サービス

説明：サービスのグループまたはプロトコル/デスティネーションポート/ソースポート。

【0024】カテゴリ名: アクション

説明: ルールアクション、例えば、「通過」、「廃棄」または「プロキシ」。

【0025】カテゴリ名: 廃棄通知

説明: YESの場合、アクションが「廃棄」であれば、インターネット制御メッセージプロトコル(ICMP)メッセージが送出される。

【0026】カテゴリ名: キャッシュタイムアウト

説明: セッションエントリがキャッシュから除去されるまでのアクティビティなしの秒数。

【0027】カテゴリ名: リセットセッション

説明: YESの場合、TCPセッションに対して、キャッシュタイムアウト時にコネクションの両端にTCPリセットを送る。

【0028】カテゴリ名: ルールタイムアウト

説明: ルールがルールリストから除去されるまでのアクティビティなしの秒数。

【0029】カテゴリ名: 開始期間

説明: ルールに対する開始アクティブ期間。

【0030】カテゴリ名: 終了期間

説明: ルールに対する終了アクティブ期間。

【0031】カテゴリ名: 期間終了時セッション消去

説明: YESの場合、このルールによって許可されたセッションは期間終了時に消去(kill)される。

【0032】カテゴリ名: 依存関係マスク

説明: 依存関係マスク名。

【0033】カテゴリ名: 入力インタフェース

説明: 受信時に一致すべきインタフェース名。

【0034】カテゴリ名: 出力インタフェース

説明: パケットが送信されるインタフェース名。

【0035】カテゴリ名: 監査セッション

説明: 監査記録生成。YESの場合、セッションの開始時および終了時に監査記録が生成される。

【0036】カテゴリ名: アラームコード

説明: ルールを特定のアラームに結び付けるために用いられるアラームコード値。

【0037】カテゴリ名: ソースホストマップグループ

説明: IPアドレス、または、マップ先のホストIPアドレスを含むホストグループ。

【0038】カテゴリ名: ソースホストマップタイプ

説明: 実行されるマッピングのタイプ(例えば、「プール」あるいは「直接」)。

【0039】カテゴリ名: デスティネーションホストマップグループ

説明: IPアドレス、または、マップ先のホストIPアドレスを含むホストグループ。

【0040】カテゴリ名: デスティネーションホストマップタイプ

説明: 実行されるマッピングのタイプ(例えば、「プール」あるいは「直接」)。

【0041】カテゴリ名: サービスマップグループ

説明: マップ先のデスティネーションポート番号またはデスティネーションポートを含むサービスグループ。参照されるサービスグループ内のプロトコルおよびソースポートは無視される。

【0042】カテゴリ名: サービスマップタイプ

説明: 実行されるマッピングのタイプ(例えば、「プール」あるいは「直接」)。

【0043】カテゴリ名: 最大使用総数

説明: このルールが使用されることが可能な最大回数。この限界に達するとルールは除去される。

【0044】カテゴリ名: 最大使用並行数

説明: 与えられた時刻にアクティブであることが可能な、このルールによって許可されるセッションの最大数。この数が、指定された値を下回るまで、ルールはイナクティブである。

【0045】カテゴリ名: コピー先アドレス

説明: パケットのコピーが送られるアプリケーションのアドレス。セッションキャプチャに用いられる。

【0046】カテゴリ名: トンネルデスティネーション

説明: トンネルを設定し、それをこのデスティネーションアドレスおよびプロトコルに送る。新しいIPヘッダがパケットに追加される。

【0047】カテゴリ名: トンネル条件

説明: トンネリングが必要となるときを示す。NULLの場合、チェックは不要である。INの場合、入力セッションはトンネリングされていなければならない。OUTの場合、パケットをトンネリングするアクションを開始する。BOTHの場合、両方を行う。

【0048】カテゴリ名: IPSEC条件

説明: IPセキュリティ(IPSEC(IP Security))処理が必要となるときを示す。NULLの場合、チェックは不要である。INの場合、入力セッションはIPSECを用いて保護されていなければならない。OUTの場合、IPSEC保護を追加するアクションを開始する。BOTHの場合、両方を行う。

【0049】カテゴリ名: シーケンス番号ランダム化

説明: TCPシーケンス番号をランダム化するオプション。デフォルトはNOである。

【0050】カテゴリ名: Syn Storm保護

説明: Syn Storm攻撃からの保護を提供する。デフォルトはNOである。

【0051】カテゴリ名: 復帰チャネル許可

説明: YESの場合、初期パケットは同じアクションでキャッシュに順チャネルおよび逆チャネルを生成する。デフォルトはYESである。

【0052】2. 状態付きパケットフィルタリング

本発明によるコンピュータネットワークファイアウォールは、「状態付き」パケットフィルタリングを利用するように設定することができる。状態付きパケットフィル

タリングは、パケットに適用されたルール処理の結果をキャッシュに記憶することによって性能を改善する。状態付きパケットフィルタリングは、受信パケットに対するルール処理結果をキャッシュし、その後、キャッシュされた結果を利用して、同様のパケットに対するルール処理を迂回することにより実現される。例えば、与えられたネットワークセッションのパケットにルールセットを適用した結果をキャッシュし、同じネットワークセッションからの後続のパケットがファイアウォールに到着したときに、前のパケットからのキャッシュされた結果をその後続パケットに対して使用するようにする。これによって、入力パケットのそれぞれにルールセットを適用する必要がなくなることにより、従来のファイアウォールに比べて大幅な性能向上が実現する。

【0053】キャッシュエントリ数はルールの数の何倍にもなり得るため、キャッシュの効率的な使用は、(例えばハッシュテーブルを用いた)索引付けを必要とすることがある。図4に示すように、キャッシュは「セッションキー」、ハードウェアアドレス情報、インタフェース情報、適用可能なルールの数、アラームコード、統計情報、および適用可能なアクションを含むことが可能である。セッションキーは、パケット内で送信されるデータに付加された少なくとも1つのヘッダ項目を含み、実施例では、(i) インターネットプロトコル(IP)ソースアドレス、(ii) IPデスティネーションアドレス、(iii) 次のレベルのプロトコル(例えば、伝送制御プロトコル(TCP)またはユーザデータグラムプロトコル(UDP))、(iv) プロトコルに関連づけられたソースポート、および(v) プロトコルに関連づけられたデスティネーションポート、を含む。図4では、セッションキーに対して、項目(i)および(ii)は個別に示されている。項目(iii)～(v)は、略して「TELNET」および「MAIL」で表されている。

【0054】ファイアウォールでは、ここで「ドメインサポートエンジン(DSE(domain support engine))」と呼ぶ判断モジュール(エンジン)が、新しいネットワークセッションに対していずれのセキュリティポリシーを使用すべきかを判断する。新しいセッションはそれぞれ、ソースドメインおよびデスティネーションドメインのセキュリティポリシーによって承認されなければならない。インターネットへ向かうコネクションでは、単一のドメインの検査のみが実行される可能性が高い。DSEは、入力または出力ネットワークインタフェースと、各パケットのソースまたはデスティネーションネットワークアドレスに基づいて、ドメイン選択を行う。ソースまたはデスティネーションのアドレスをパケットに含めることにより、複数のユーザが、単一のネットワークインタフェースによってサポートされることが可能となる。入力または出力ネットワークインタフェースは、ネ

ットワークインタフェースカード(NIC)(例えばインテル社(Intel Corporation)から市販されているIntel EtherExpress Pro 100Bカード)の形態のものが可能である。

【0055】図5および図6は、複数のドメインをサポートするファイアウォールによるパケット処理の全体流れ図である。このような処理は、パケットが行くドメインを判断し、適用可能なルールを検査してパケットが通ってもよいかどうかを確認し、特殊処理が必要稼働かを判断することを含む。ファイアウォールでは、各ドメインには1つ以上のネットワークインタフェースが関係づけられる。複数のドメインをサポートするインタフェースは、IPアドレスレンジを用いて、パケットを区別するように分離される。以下のステップが含まれる。

【0056】501: IPパケットがインタフェースでファイアウォールにより受信される。

【0057】502: パケットのIPヘッダからセッションキーが取得される。

【0058】503: いずれのインタフェースがパケットを受信したか、および、受信パケットのソースIPアドレスに基づいて、ソースドメインが、図7および図8に関して別に後述するように判定される。ドメインが見つからない場合、プロセスはステップ505に飛ぶ。

【0059】504: ステップ502からのセッションキーを用いて、ソースドメインのキャッシュでの一致を探索する。キャッシュ内に一致があり、アクションが「廃棄」の場合、パケットは廃棄され、プロセスはステップ501に戻る。キャッシュ内に一致がない場合、ソースドメインのルールセットで一致を探索する。ルールで一致があり、アクションが「廃棄」でない場合、プロセスはステップ505に進む。ルールで一致があり、アクションが「廃棄」の場合、対応するエントリがキャッシュに含められ、パケットは廃棄され、プロセスはステップ501に戻る。ルールで一致がない場合、パケットは廃棄され、プロセスはステップ501に戻る。

【0060】505: パケットのローカルエリアネットワーク(LAN)アドレスを用いて、しかも、ソースドメインルールがデスティネーションインタフェースを指定している場合には、そのデスティネーションインタフェースおよびルーティングテーブルを用いて、デスティネーションインタフェースが決定される。

【0061】506: デスティネーションインタフェースおよびパケットのデスティネーションアドレスを用いて、デスティネーションドメインが決定される。デスティネーションドメインが見つからない場合、または、デスティネーションドメインが直前に検査したドメインと一致する場合、プロセスはステップ508に進む。

【0062】507: ソースドメインに関してステップ504で用いられるのと同様にして、デスティネーションドメインに関して、キャッシュルックアップと、必要

であればルールセットルックアップを行う。

【0063】508：パケットに適用されるルールがアドレス変更（例えば、プロキシへの）を要求する場合、あるいは、あるパケットを別のパケット内に挿入すること（「トンネルオプション」）を要求する場合、プロセスは、変更されたデスティネーションに基づく処理のためにステップ505に戻る。

【0064】509：パケットがいずれのドメインに関しても処理されなかった場合、ファイアウォール所有者はいずれのアクセスルールにも従わないインタフェース間の通信をサポートすることには関心がないので、そのパケットは廃棄可能である。

【0065】510：すべてのアクションの結果が「通過」であった場合、パケットは適当なネットワークインタフェースへ送出される。

【0066】各ネットワークインタフェースからドメインへの簡便なリンクのために、ドメインテーブルが用いられる。インタフェースが複数のドメインによって共有されている場合、アドレスレンジが含まれる。これは図7に例示されている。図7には、重複のないアドレスレンジが示されている。

【0067】図8に、上記のステップ503および506で実行されるようなドメインテーブル処理を例示する。これには以下のステップが含まれる。

【0068】701：ドメインテーブルでインタフェース名が一致するものを探索する。

【0069】702：一致するテーブルエントリが見つかった場合、しかも、IPアドレスレンジが一致するテーブルエントリにある場合、パケットアドレスがそのレンジ内にあるかどうかを検査する。レンジ内にある場合、指定されたドメインが選択される。レンジ内にない場合、次のテーブルから探索を継続する。

【0070】703：一致するものがないままテーブルの終端に到達した場合、何のアクションもとらない。

【0071】3. 依存関係マスク

例えばRealAudioによって用いられるプロトコルのような、外部からユーザに戻る別個の追加のネットワークセッションを要求するタイプのプロトコルの場合、ルールは、ユーザに戻るコネクションを許可する条件あるいはマスクを含むことが可能である。ただしそれは、並行してアクティブである正当な順方向のコネクション（すなわち、ソースとデスティネーションのアドレスを入れ替えたコネクション）がある場合に限る。その結果、ファイアウォール上に別個のあるいはプロキシのアプリケーションが不要となる。

【0072】本発明による依存関係マスクは、セッションキャッシュに向けられた問合せを定義することができる。マスクで定義されるすべてのフィールドを、キャッシュ内の対応するフィールドと比較することによって、一致の有無が判定される。マスク内の空フィールドは比

較に用いられない。

【0073】依存関係マスクは、（a）パケット内の情報、（b）そのパケットのソースインタフェース、および（c）そのパケットが通過するために満たさなければならない1つまたはいくつかの依存条件、を用いて、ネットワークセッションの最初のパケットに対するルールで定義することが可能である。このような最初のパケットがファイアウォールによって処理されると、対応するエントリがキャッシュに作られる。

【0074】図9に、図3のものと同様のフォーマットで、依存関係マスク（「ヒットカウント」）を有するルールを示す。以下のような特殊な記号が、いくつかのホスト名にある。（i）「ドット」記号（.）は、対応するカテゴリのパケットデータを含めることを要求し、（ii）キャレット記号（^）は、代わりに異なるカテゴリからのパケットデータを含めることを要求する。

「ヒットカウント」は、指定されたアクションがとられるためにキャッシュ内に見つからなければならない一致の数を示す。例えば、「REALAUDIO」という名前の依存関係マスクでは、1個の必須のTCPセッションがアクティブである限り、UDPパケットを通過させるためにはカウント1が用いられる。依存関係マスク「TELNET」では、リソースの過負荷を防ぐためにパケットを廃棄するように、カウント10が用いられる。

【0075】図10に依存関係マスク処理を例示する。これは以下のステップを含む。

【0076】901：パケットを取得し、セッションキーを抽出する。

【0077】902：プロセスはルールセットエントリを順に処理する。与えられたルールで一致が見つからない場合、プロセスはセット内の次のルールに進む。ルールセットの終端まで一致が見つからない場合、パケットは廃棄される。一致が見つかり、依存関係マスクフィールドが空の場合、プロセスはステップ905に飛ぶ。

【0078】903：パケットおよびインタフェース情報が、キャッシュ探索構造体（例えば、問合せ）の形成に含められる。依存関係マスクにおいてユーザ認証フラグがセットされている場合、キャッシュ探索構造体における対応するフラグがセットされる。このステップは、ルールの問合せ部分を定義している。

【0079】904：キャッシュで、キャッシュ探索構造体と一致するものを探索し、一致のカウントを積算する。このステップは、ルールの問合せ部分を処理している。

【0080】905：積算カウントがヒットカウント以上である場合、ルールは選択され、そのルールに対応するアクションが実行される。このようなアクションは、通過、廃棄あるいはプロキシを含むことが可能である。また、対応するエントリがキャッシュに作られる。キャ

ッシュにおいて一致が見つからない場合、または、キャッシュに見つかったエントリが「ヒットカウント」より少ない場合、プロセスはステップ902に戻り、次のルールに進む。このステップは、問合せの結果に基づいてルールのアクション部分を処理している。

【0081】上記の依存関係マスク処理を含むルール処理は、ネットワークセッションの最初のパケットに対してのみ実行される。他のすべてのパケットのアクションは、最初のパケットの処理後にセッションキャッシュに保存されているので、他のすべてのパケットは、このルール探索機能を迂回する。

【0082】4. 動的ルール

動的ルールは、例えばルール処理エンジンによって、アクセスルールとともに処理するために、必要が生ずるのに応じてアクセスルールとともに含められるルールである。動的ルールは、例えば、特定のソースおよびデスティネーションのポート番号のような、固有の現在の情報を含むことが可能である。動的ルールは、信頼されたパーティ、例えば、信頼されたアプリケーション、リモートプロキシあるいはファイアウォールアドミニストレータによって、特定のネットワークセッションに権限を与えるためにいつでもロードされることが可能である。動的ルールは、単一セッション用に設定されることも可能であり、あるいは、その使用は期限付きとすることも可能である。動的ルールによれば、ルールセット全体をリロードすることを要求することなく、与えられたルールセットを、ネットワークで起こるイベントに基づいて修正することが可能となる。

【0083】動的ルールの例としては、単一のセッションに対してのみ用いられる「ワンタイム」ルール、指定された期間に対してのみ用いられる時限ルール、および、ある条件が満たされたときにのみ用いられるしきい値ルールがある。他のタイプの動的ルールとしては、ホストグループを定義するルールがある。この動的ルールによれば、アクセスルールセットの他の事項を変更せずに、ホストを追加あるいは削除するようにホストグループを変更することができる。他の動的ルールとしては、ある特定のタイプの処理アプリケーションにおけるルールセットアップを容易にするために用いられるものがある。例えば、FTPプロキシアプリケーションは、動的ルールを用いて、データ要求に応じてFTPデータチャネルの確立の権限を与えることが可能である。この例における動的ルールは、一般に、FTP制御セッションを通じてデータ要求がなされるまではロードされず、また、1回の使用に限定され、制限された期間の間のみアクティブとされる。従って、ルールセットは、すべての要求とともに用いられる別個のデータチャネルルールを含む必要がない。その結果、ルール仕様およびルール処理が単純化されるとともに、セキュリティが改善される。

【0084】5. プロキシ反射

本発明によるプロキシ反射とは、ネットワークセッションを、処理のために他の「リモート」プロキシサーバにリダイレクトした後、ファイアウォールを通じて目的のデスティネーションへ渡すものである。新しいセッションがファイアウォールに入ると、プロキシサーバによるサービスが要求されているかどうかが判定される。プロキシサーバによるサービスが要求されている場合、ファイアウォールは、パケット内のデスティネーションアドレスを、プロキシアプリケーションのホストアドレスで置き換える。必要であれば、ファイアウォールは、サービスポートも変更することが可能である。プロキシアプリケーションは、そのセッションを受け取ると、デスティネーションへのコネクションの権限が与えられているかどうかを判定するために、ファイアウォールに対して、そのセッションのものとデスティネーションアドレスを要求する。その後、プロキシが、自己のIPアドレスを用いてそのデスティネーションへのコネクションを形成する場合、ファイアウォールによって提供されるサービスを「単一反射」あるいは「一方向反射」という。

【0085】ユーザおよびプロキシアプリケーションによっては、デスティネーションにおいてコネクションがリモートシステムではなくもとのソースから来ているように見えなければならない場合がある。これは、例えば、ソースIPアドレスを検査して、要求されたサービスに対してサインアップしたユーザに一致するかどうかを確認するサービスの場合に当てはまる。この能力は、「二重反射」（あるいは「双方向反射」）によって提供される。この場合、出コネクションのソースアドレスはリモートプロキシからもとのユーザのソースアドレスに変更される（戻される）。この変更は、各パケットがプロキシから受信されてデスティネーションへ送られるときに、ファイアウォールで行われる。

【0086】二重反射能力を提供するため、プロキシアプリケーションは、ファイアウォールに対して、もとの入ネットワークセッションの詳細を要求する。ファイアウォールは、出コネクションで用いるポート番号を返す。このポート番号は固有のものであり、これによりファイアウォールは、ソースアドレスを正しいユーザソースアドレスにマッピングすることができるようになる。正しい出コネクションを識別することができる。その結果、プロキシアプリケーションは両方のパーティには見えない。

【0087】プロキシ反射を実現する際に、図11および図12を参照して以下で説明する実施例のように、動的ルールを用いることが可能である。

【0088】図11に、プロキシ反射処理を例示する。これは、ファイアウォールにおける以下のステップを含む。

【0089】1001：パケットがファイアウォールに

よって受信される。

【0090】1002：適当なセッションキャッシュを調べることによって、あるいは、キャッシュ内に見つからなければ、適当なルールセットを調べることによって、パケットに関係づけられたアクションが判定される。アクションが「通過」または「プロキシ」である場合、パケット処理は継続される。アクションが「廃棄」である場合、パケットは廃棄される。

【0091】1003：アクションが、ファイアウォール上でローカルにサポートされるプロキシアプリケーションを示している場合、パケットは、プロトコルスタックを通じて、待機中のプロキシアプリケーションへ送られる。

【0092】1004：アクションがリモートプロキシを示している場合、パケットのデスティネーションアドレスがリモートプロキシのアドレスで置き換えられる。設定により、デスティネーションポートを変更することも可能である。もとのパケットヘッダデータが、変更された値とともにセッションキャッシュに記録される。

【0093】1005：パケットはリモートプロキシサーバへ転送される。

【0094】図12に、リモートプロキシにおける、ステップ1005に続く処理を例示する。これは以下のステップを含む。

【0095】1006：パケットはリモートプロキシサーバアプリケーションで受信される。

【0096】1007：リモートプロキシは、ファイアウォールに対して、パケットのもとのセッションキーを要求する。

【0097】1008：リモートプロキシアプリケーションは、もとのセッションキーを用いて自己の機能（例えば、自己のセキュリティモデルに基づいてコネクションを廃棄する、要求されたサービスを実行する、あるいは、ユーザに代わってもとのデスティネーションアドレスと通信する）を実行する。リモートプロキシが単一反射を用いている場合、プロセスはステップ1011に飛ぶ。

【0098】1009：リモートプロキシアプリケーションは、暗号化されたチャンネルを通じて、ファイアウォールに対して二重反射能力を要求する。

【0099】1010：ファイアウォールは、サーバからのコネクションの固有性を保証する新しいデスティネーションポート番号を決定する。ファイアウォールはこの新しいポート番号およびもとのセッションキーをプロキシアプリケーションに返す。

【0100】1011：リモートプロキシアプリケーションは、ファイアウォールに対して、自己からもとのデスティネーションへのコネクションに対する許可を要求する。

【0101】1012：ファイアウォールは、動的ルー

ルをロードしてこのアクションを実行する。

【0102】1013：リモートプロキシは、パケットをファイアウォールに送る。ステップ1012でロードされた動的ルールに基づいて、ファイアウォールはパケットをもとのデスティネーションへ転送する。二重反射の場合、プロキシは、ステップ1010でファイアウォールによって決定されたデスティネーションポートを使用し、パケットがファイアウォール通過するときに、IPヘッダ値はもとの値に戻される。

【0103】同じセッションに関係づけられた後続のすべてのパケットは、ステップ1007および1009～1012を飛ばすことが可能であることを除いては、同様に処理される。これは、セッションが生きている間、同じ動的ルールが適用されるからである。

【0104】本発明は、広範囲のアプリケーションで実施することができる。例えば、本発明は、ダイヤルアップアクセスゲートウェイにおけるファイアウォール性能を改善するために使用可能である。本発明の別の実施例では、ファイアウォールの第1部分がネットワークに存在し、ファイアウォールの第2部分がセットトップボックス、コンピュータあるいはその他の、家庭または会社にあるユーザ端末にあるというように分散的にも実装可能である。後者の実施例によれば、本発明のファイアウォール技術は、例えば、家庭においてインターネットとビデオアクセスの親による制御を提供することが可能である。

【0105】

【発明の効果】以上述べたごとく、本発明によれば、複数のセキュリティドメインをサポートする能力により、単一のファイアウォールが、それぞれ別々のセキュリティポリシーを有する複数のユーザをサポートすることが可能となる。また、相異なるセキュリティポリシーをサブサイト間の通信に適用することができるため、このような能力は、サイト内でも使用可能である。

【図面の簡単な説明】

【図1】ユーザサイトに対するファイアウォール保護を提供するローカルエリアネットワークを通じてインターネットに接続されたいくつかのユーザサイトあるいはドメインの図である。

【図2】インターネットに接続され内部ファイアウォールを有するユーザサイトの図である。

【図3】ルールテーブルを例示する図である。

【図4】キャッシュを例示する図である。

【図5】複数のドメインに対するファイアウォール処理の全体流れ図である。

【図6】複数のドメインに対するファイアウォール処理の全体流れ図である。

【図7】ドメインテーブルを例示する図である。

【図8】複数のドメインに対するファイアウォール処理の一部の流れ図である。

【図9】依存関係マスクを例示する図である。

【図10】依存関係マスク処理の流れ図である。

【図11】ファイアウォールにおけるプロキシ反射処理の流れ図である。

【図12】リモートプロキシにおけるプロキシ反射処理の流れ図である。

【符号の説明】

101 ユーザサイト

102 ユーザサイト

103 ユーザサイト

104 ユーザサイト

105 インターネット

110 LAN

111 ファイアウォールプロセッサ

113 ファイアウォールプロセッサ

114 ファイアウォールプロセッサ

115 アドミニストレータプロセッサ

116 ルータ

117 ウェブサーバ

201 ユーザサイト

211 ファイアウォールプロセッサ

212 ファイアウォールプロセッサ

213 ファイアウォールプロセッサ

215 アドミニストレータプロセッサ

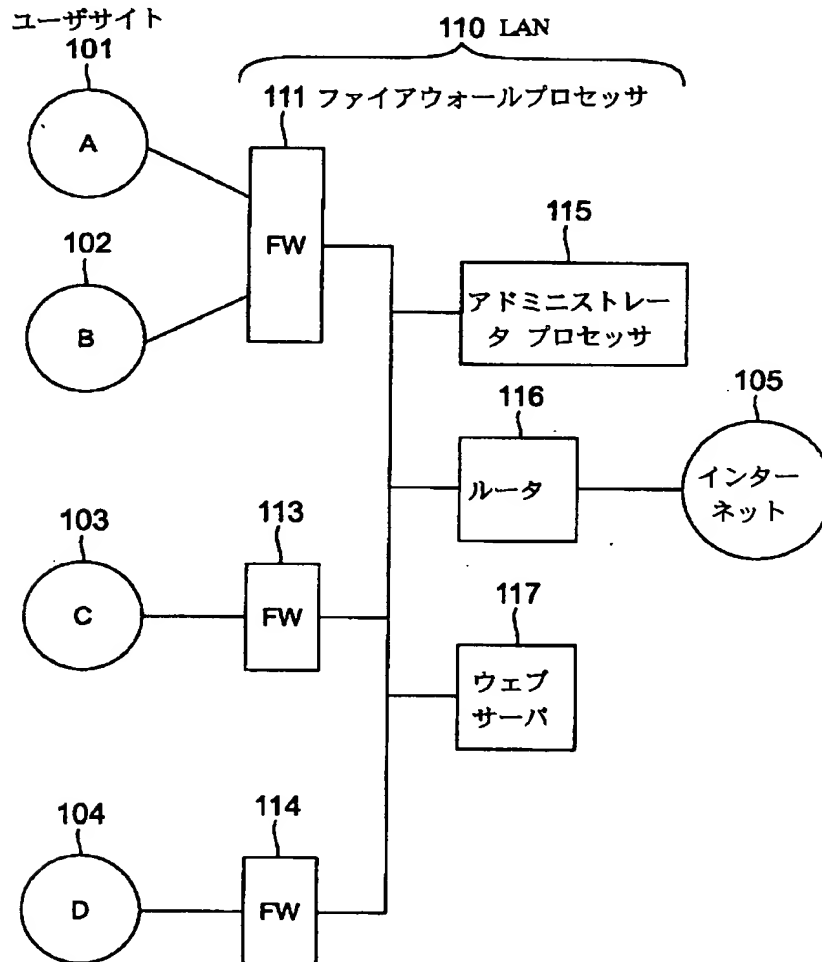
216 ルータ

221 サブサイト

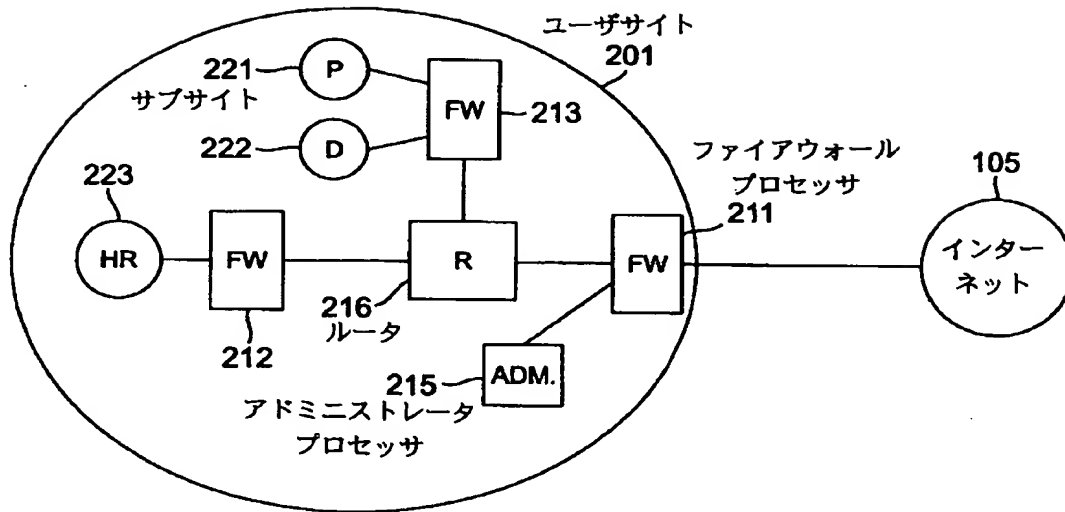
222 サブサイト

223 サブサイト

【図1】



【図2】



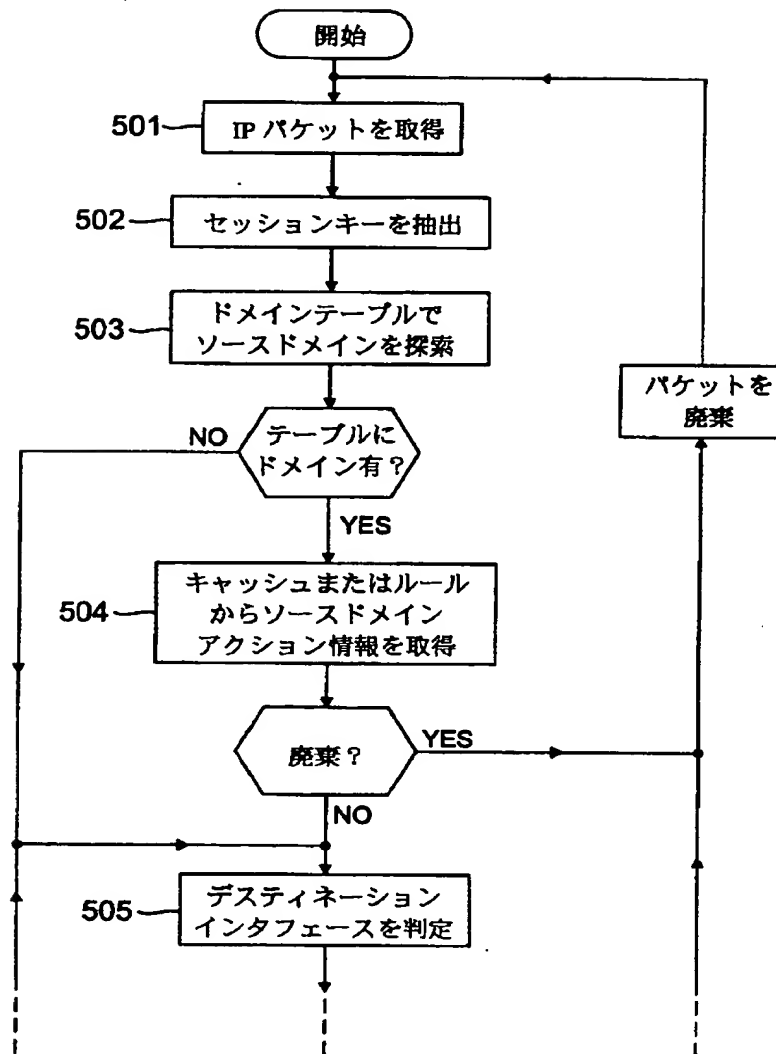
【図3】

ルール番号	ソース ホスト	デスティネーション ホスト	サービス	アクション
10	A	B	FTP	通過
20	A	*	*	廃棄
30	B	C	TELNET	プロキシ
40	*	D	MAIL	通過

【図4】

セッション キー	ハード ウェア アドレス	インタ フェース	ルール 番号	アラーム コード	統計情報	アク ション
A, B, TELNET	Ma, Mb	en0, en1	10	10	5 パケット	通過
B, A, TELNET	Mb, Ma	en1, en0	10	10	5 パケット	通過
C, A, MAIL	Mc, Ma	en1, en0	30	20	100 パケット	通過
A, C, MAIL	Ma, Mc	en0, en1	30	20	10 パケット	通過
D, A, TELNET	Md, Ma	en1, en0	40	30	15 パケット	廃棄
E, A, MAIL	Me, Ma	en1, en0	30	10	30 パケット	通過
A, E, MAIL	Ma, Me	en0, en1	30	10	10 パケット	通過

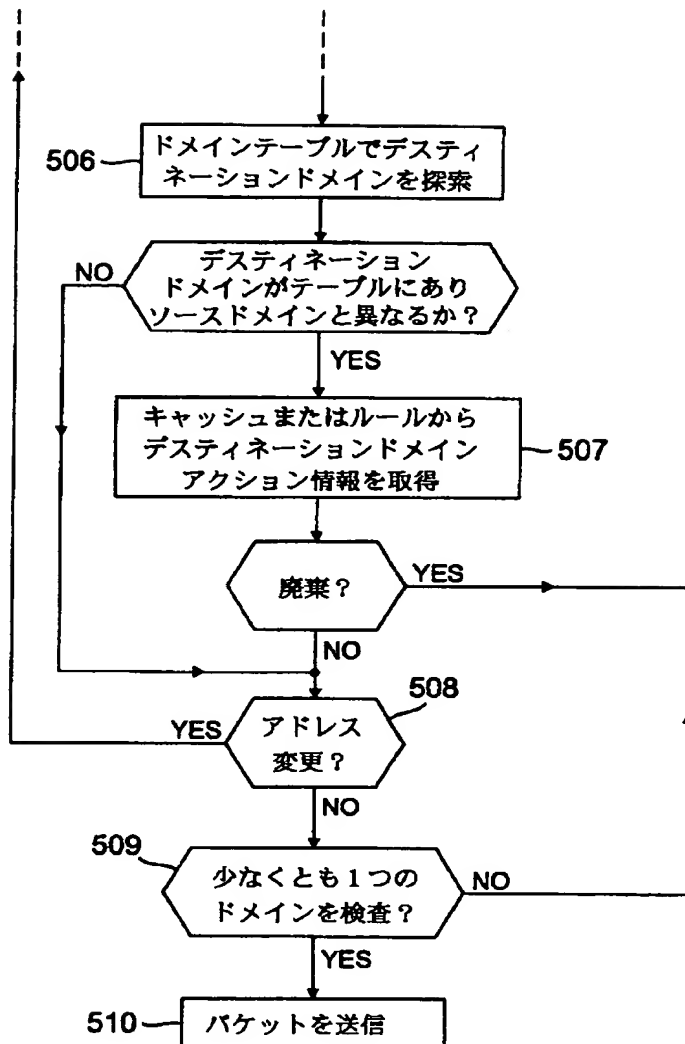
【図5】



【図7】

インタフェース	アドレスレンジ	ドメイン
0	10.50.0.0 - 10.50.255.255	A
0	10.60.0.0 - 10.60.255.255	B
1	*	C
2	*	*

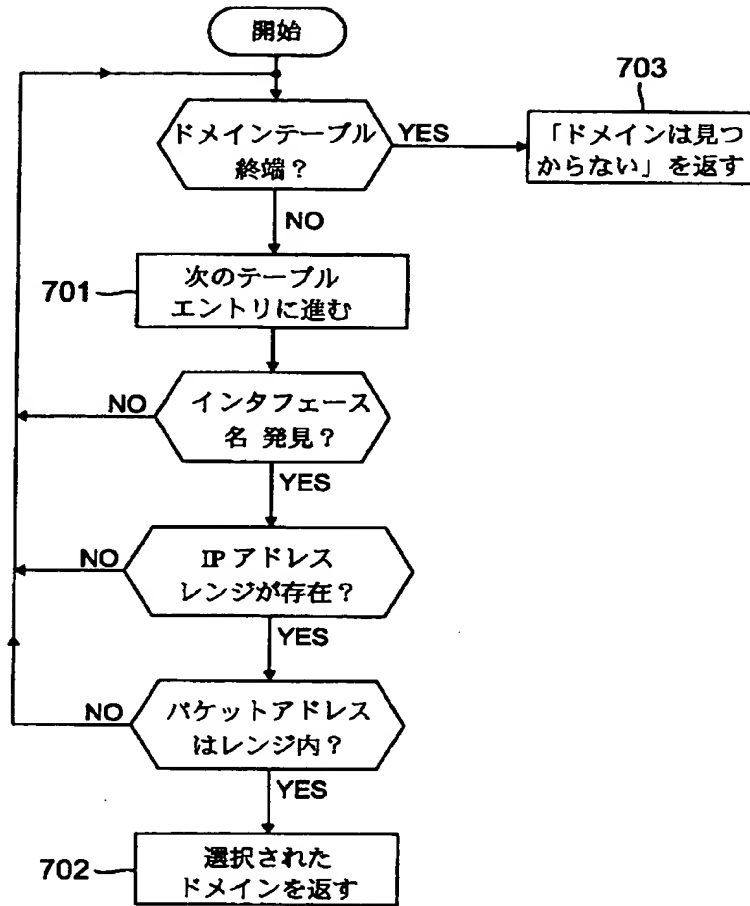
【図6】



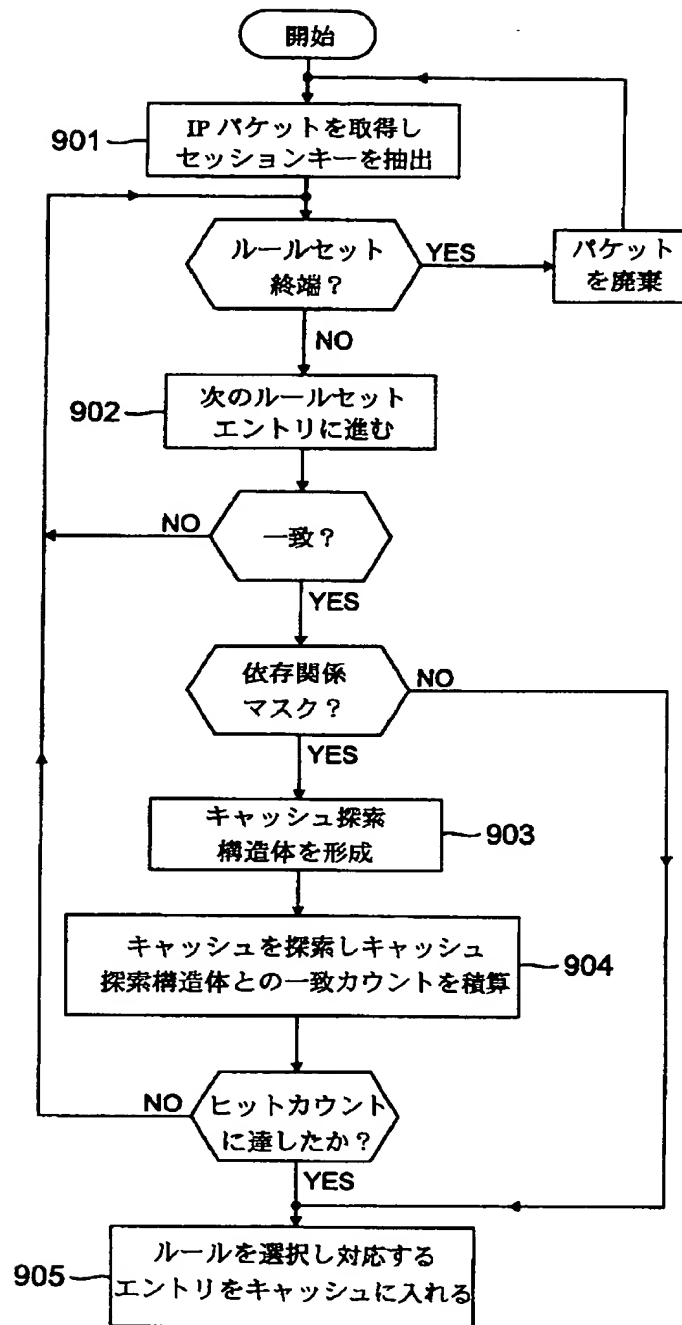
【図9】

名称	ソース ホスト	デスティ ネーション ホスト	サービス	アクション	ヒット カウント
TRACEROUTE	^	*	TRACEROUTE	通過	1
PPTP	.	.	TCP/1723	通過	1
TELNET	A	B	TELNET	廃棄	10
REALAUDIO	^	*	TCP/7070	通過	1

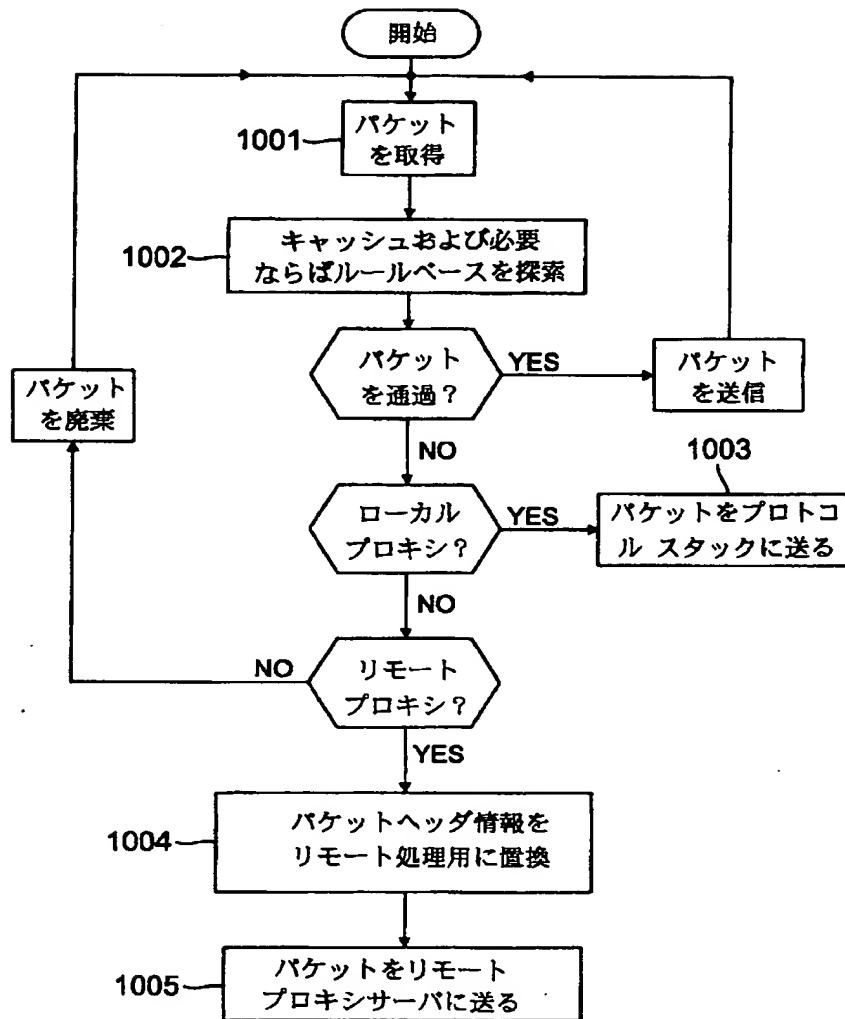
【図8】



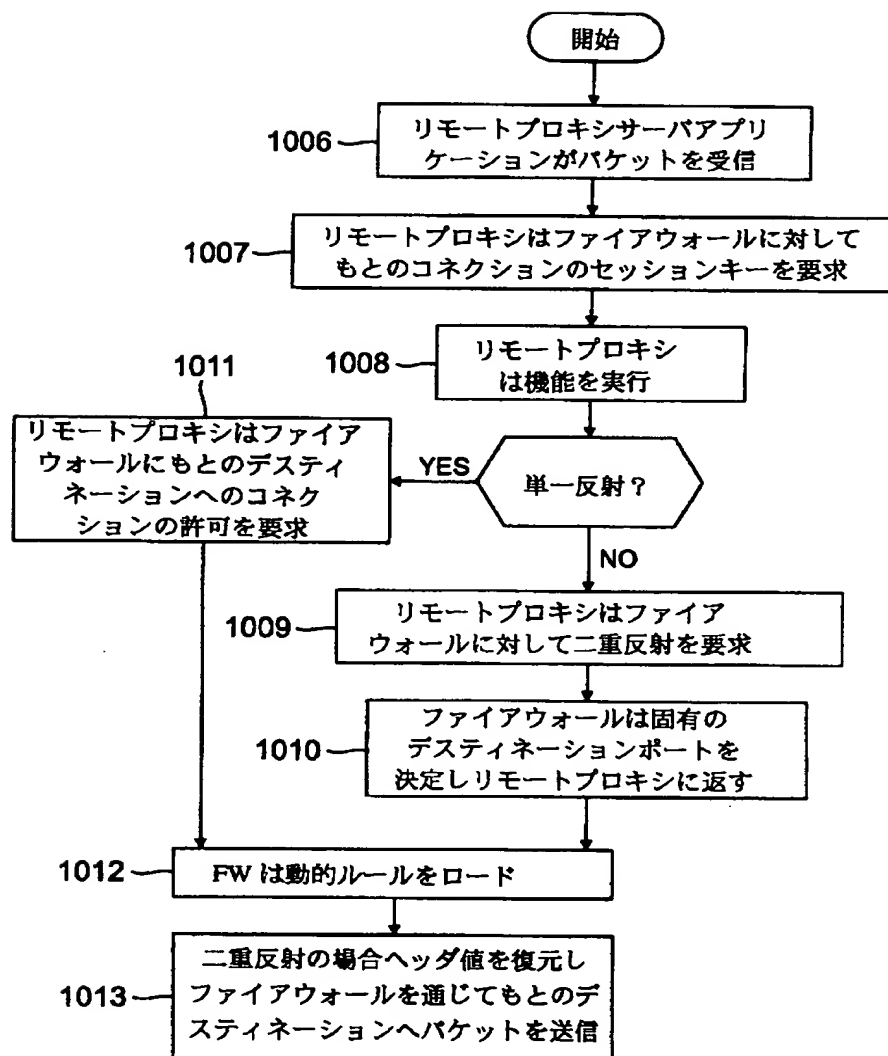
【図10】



【図11】



【図12】



フロントページの続き

(71)出願人 596077259
600 Mountain Avenue,
Murray Hill, New Jersey 07974-0636 U. S. A.

(72)発明者 デヴィッド エル. マジェット
アメリカ合衆国, 07924 ニュージャージー,
バーナーズヴィル, マレンズ レイン
73

(72)発明者 ロナルド エル. シャープ
アメリカ合衆国, 07830 ニュージャージー,
キャリフォン, ギャリー レイン, レ
イルロード2 ボックス 245